eduroam Operations Team

Admin Advisory-003

Cipher suite selection for eduroam Service Providers

Summary of issue

- Date of disclosure: 06 November 2008.
- A weakness has been found in TKIP network encryption (WPA/TKIP and WPA2/TKIP).
- Risk level is currently low but likely to increase.
- Suggested solution: Enable AES support, educate users to migrate clients to WPA2/AES.
- Impact of solution: Wireless access points may need to be upgraded/replaced. Client devices may need to be reconfigured and/or supplicant software upgraded/replaced.

Detailed issue analysis and recommendations

Recent research[1] has revealed a method to partially compromise WPA-TKIP and WPA2-TKIP encrypted networks, enabling the extraction of data and injection of forged data. Currently only a few packet types and small amounts of data can be extracted and altered, and the encryption key is not compromised, so the immediate security impact is limited. However, this security threat could be developed and exploited in the future.

Because the provisioning of a wireless network is a long-term investment and of strategic importance, the potential for future attacks against TKIP must be taken into account. Therefore, the eduroam Operations Team recommends that new eduroam Service Provider site deployments do not employ TKIP as their encryption algorithm., and that TKIP should be considered a legacy encryption method.

Existing deployments need not take immediate action to migrate from TKIP encryption, but should be aware that this should be considered and planned in an appropriate time frame (for example when equipment is due for renewal).

The recommended migration is to AES encryption. This Advisory notice gives eduroam Service Providers information on possible migration paths from TKIP to AES encryption, depending upon their current deployment.

New deployments

If you are deploying a new eduroam Service Provider, you should provide WPA2/AES **only**. As all older encryption schemes either display a cryptographic compromise (WEP, WPA/TKIP, WPA2/TKIP) or have limited client compatibility (WPA/AES), it is not advisable to introduce such legacy ciphers in new site deployments.

Existing deployments

WPA/TKIP and WPA2/AES

In this instance the network already offers WPA2/AES as an option, and therefore action is not necessary. In this case you are advised to inform your users about the new shortcomings of WPA/TKIP and encourage them to use WPA2/AES only. You can then maintain your setup as it stands.

However, if you are concerned about your network security and want to remove the WPA/TKIP cipher you may do so, but keep in mind that moving to WPA2/AES only may leave some users behind:

- Users who currently use WPA/TKIP and cannot use WPA2/AES. will not be able to use the service after WPA/TKIP is removed. You are advised to carry out the migration to AES and either advise these users to upgrade their networking equipment as soon as possible (but survey these upgrades to be aware of any potential impact), or provide them with a legacy SSID that allows WPA/TKIP usage. This SSID should not have the brand name “eduroam” in its name, and should not allow any roaming access (i.e.: a service for local legacy users only). Please be aware that the international eduroam policy will be revisited due to the TKIP compromise, and that TKIP ciphers may become officially discontinued – which implies that the usage of the brand name “eduroam” for WPA/TKIP networks may become forbidden at a later stage.
- Users who currently use WPA/TKIP and, although able to use AES, are unwilling to upgrade. To continue using eduroam after the AES upgrade, these users must reconfigure their clients (which could increase helpdesk load).

If you choose not to move to WPA2/AES exclusively, please read the section “Re-keying interval considerations” on page 3.

WPA2/AES only

Deployments with WPA2/AES encryption exclusively do not need to take any action.

WPA/TKIP only

You should examine your site hardware and firmware to find out whether it is possible to enable WPA2/AES in addition to WPA/TKIP in a mixed mode (for example with a firmware upgrade). If possible, you should take the necessary steps to enable WPA2/AES in addition to WPA/TKIP. At that point, consult the section above for Service Providers with WPA/TKIP and WPA2/AES for further security considerations.

Note: Some clients with broken supplicants may get confused by the presence of WPA/TKIP and WPA2/AES in a network at the same time.

If your equipment does not allow you to use WPA2/AES, you should consider acquiring a new generation of wireless networking equipment and upgrade your network to a mixed mode WPA/TKIP and WPA2/AES. If upgrading your equipment is not an option right now, you may continue to use your setup as it is now. Please be aware that the international eduroam policy will be revisited due to the TKIP compromise, and that TKIP ciphers may become officially discontinued – which implies that the usage of the brand name “eduroam” for WPA/TKIP networks may become forbidden at a later stage.

If you choose not to move to WPA2/AES, please read the section “Re-keying interval considerations” on page 3.

Other ciphers

WPA/AES: This is is a rather unusual setting, and is not affected by the TKIP vulnerability. You do not need to take any action. If you choose not to move to WPA2/AES, please read the section “Re-keying interval considerations” on page 3.

WPA2/TKIP: This is both rather unusual and compromised. We suggest configuring WPA2/AES instead. Some client devices may be left behind by this measure.

Dynamic WEP: This is discouraged in eduroam due to severe and long-standing security problems. While the attack referenced in this advisory shows new ways of compromising TKIP, the same principles are also applicable to WEP encryption. If you still have WEP-only equipment, we very strongly suggest you upgrade to a new generation of wireless networking equipment that supports modern encryption settings (like WPA2/AES). Furthermore, as the move from WEP to any one of WPA or WPA2 is a client configuration-intensive leap anyway, we suggest to move on to WPA2/AES in one big step. Note that there are still client devices with very old legacy hardware that is unable to use WPA2/AES or WPA/TKIP. You can choose to either leave this user group behind and demand them to upgrade their wireless networking hardware (we strongly suggest to survey your site before doing so, to become aware of the potential impact) or to provide a legacy network that enables WEP usage. Please note that Dynamic WEP is already below the minimum security recommendations in the current European eduroam Confederation policy, and may become forbidden in a future revision of the policy. Because of that, it is not advised to use an SSID containing the brand name "eduroam" for this network, to prevent a later required SSID change if the corresponding policy changes come into effect.

Re-keying interval considerations

If the migration to WPA2/AES is not immediately possible for whatever reasons, several measures can be taken to limit the extent of any potential attack. Several vendors provide best practices documents for their equipment (such as Aruba[2] and Cisco[3]), and you should consult the relevant documentation for your equipment to carry out any preventative procedures.

However, there are known side-effects to some of the proposed countermeasures. These are described below. Please read these carefully, as it may well be that in your concrete deployment scenario, the cure might be worse than the disease.

- Changing encryption keys during a session ("re-key")
  Some devices do not properly support re-key operations. These clients will lose connectivity when the key refresh interval is reached. All vendor recommendations propose very short re-keying intervals, for example 120 seconds. Losing connectivity in such small intervals is a severe degradation of service, and may lead to reduced satisfaction of users of such devices, as well as more helpdesk traffic.
- Re-Authenticating in short intervals
  It is not necessary to re-authenticate a user to refresh network keys. However, some equipment vendors do not support re-keying without re-authentication. An international roaming authentication in eduroam takes approximately two seconds. For the duration of the re-authentication, the client device may or may not have connectivity. This is a minor degradation of service and may lead to disgruntled users.
- Modifying countermeasure timing in TKIP
  Setting the countermeasure time in TKIP above the protocol default of 60 seconds may lead to a higher rate of discovered attacks (attackers will assume the channel is safe to use after 60 seconds, while the equipment still is in an alerted state). Unfortunately, every discovered attack leads to all TKIP clients being disconnected from the network for 60 seconds. Therefore, one attacker can create a denial of service condition for every network user. On mixed WPA/TKIP and WPA2/AES networks, there have been reports of at least one vendor that also disconnects the WPA2/AES users from the network for 60 seconds, even though this is not required. Such equipment exposes more users to a denial of service than is necessary.
  Setting the countermeasure time in TKIP below the protocol default of 60 seconds leads to faster attacks, since the attacker can retry sending packets earlier.

References

[1] http://dl.aircrack-ng.org/breakingwepandwpa.pdf
[2] https://edge.arubanetworks.com/article/tkip-vulnerabilities
[3] http://www.cisco.com/warp/public/707/cisco-sr-20081121-wpa.shtml